IT Disaster Recovery and Business Resumption Planning Policy

Adopted by the Information Services Board (ISB) on May 28, 1992
Policy No: 500-P1 Also see: 501-S1, 502-G1
Supersedes No: N/A
Effective Date: July 1, 1993
Revision Date: April 2002 Definitions

Table of Contents

Purpose

The purpose of this policy is to ensure that information technology (IT) resource investments made by agencies of the executive and judicial branches of state government are protected against service interruptions, including large scale disasters, by the development, implementation, and testing of disaster recovery/business resumption (DR/BR) plans.

Each agency must be able to demonstrate the ability to continue to provide mission-critical, IT-dependent services during recovery from a business interruption or service outage.

For purposes of this policy "disaster recovery/business resumption planning" includes, but is not limited to, the documentation, plans, policies, and procedures that are required to restore normal operation to a state agency impacted by man-made or natural outages or disasters.

The three principal goals of disaster recovery/business resumption planning are to:

- Save data.
- Save hardware, software, and facilities.
- Resume critical processes and restore data.

The policy will assist agencies to:

- Identify IT resources that are at risk.

- Implement useful plans to protect against identified threats and mitigate risk.
- Implement tested emergency procedures when a service outage occurs.
- Implement and test procedures that enable short-term recovery of IT services following a service outage.
- Develop a plan that will enable full recovery and the resumption of normal operations.

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards and procedures.

Scope

This policy applies to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

The scope includes, but is not limited to:

- Agencies that operate, manage, or use stand-alone, shared, or network-attached computers, whether mainframes, servers, or personal computers for their own use or for use by other agencies.
- Agencies that operate, manage, or use voice, data, or video telecommunications equipment, networks, or services for their own use or for use by other agencies.
- Agencies that purchase computer services or telecommunications network services from other state agencies or commercial concerns.

Exemptions

None.

Policy

Each agency shall:

1. **Develop disaster recovery/business resumption plans.** Agencies dependent on voice telecommunications, data telecommunications, video telecommunications, or computer services for carrying out their missions must develop disaster recovery/business resumption plans. Each agency is responsible and accountable for its own disaster recovery/business resumption program. Agencies that purchase computer services or telecommunications services from other state agencies or commercial concerns shall integrate their disaster recovery/business resumption plans, including off-site storage of data, with the service providers' plans.

2. **Maintain and update disaster recovery/business resumption plans annually.** Agencies shall update disaster recovery/business resumption plans at least annually and following any significant change to their computing or telecommunications environment.

3. **Test disaster recovery/business resumption plans annually.** Agencies are required to test their plan at least once a year. Agencies shall correct any deficiencies revealed by the test. The type and extent of testing adopted by an agency will depend on:
   - Criticality of agency business functions.
   - Cost of executing the test plan.
   - Budget availability.
   - Complexity of information system and components.

4. **Train their employees to execute the recovery plans.** Training will consist of:
   - Making employees aware of the need for a disaster recovery/business resumption plan.
   - Informing all employees of the existence of the plan and providing procedures to follow in the event of an emergency.
   - Training all personnel with responsibilities identified in the plan to perform the disaster recovery/business resumption procedures.
   - Providing the opportunity for recovery teams to practice disaster recovery/business resumption skills.

5. **Annually certify the updating and testing of the disaster recovery/business resumption plan.** Pursuant to RCW 43.105.017(3), agency heads are responsible for the oversight of their respective agency's management and use of IT resources. An annual disaster recovery/business resumption plan confirmation letter must be included in the agency IT portfolio and submitted to the Board by August 31 of each year. By way of this letter, the head of each agency confirms to the Board that a disaster recovery/business resumption plan has been reviewed, updated, and tested.

The State Auditor may audit disaster recovery/business resumption plans.
The State Auditor may audit agency disaster recovery/business resumption plans and tests for compliance with policy and standards.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.